

# EXTENSIONS OF CM ELLIPTIC CURVES AND ORBIT COUNTING ON THE PROJECTIVE LINE

JULIAN ROSEN AND ARIEL SHNIDMAN

**ABSTRACT.** There are several formulas for the number of orbits of the projective line under the action of subgroups of  $\mathrm{GL}_2$ . We give an interpretation of two such formulas in terms of the geometry of elliptic curves, and prove a more general formula for a large class of congruence subgroups of Bianchi groups. Our formula involves the number of walks on a certain graph called an isogeny volcano. Underlying our results is a complete description of the group of extensions of a pair of CM elliptic curves, and of a pair of lattices in a quadratic field.

## 1. INTRODUCTION

We begin with some motivation from two well-known and elegant formulas. The first formula is for the number of orbits of  $\mathbb{P}^1(\mathbb{Q})$  under the action of the congruence subgroup  $\Gamma_0(N) \subset \mathrm{GL}_2(\mathbb{Z})$ ,<sup>1</sup> acting by fractional-linear transformation:

$$(1.1) \quad \#\Gamma_0(N) \backslash \mathbb{P}^1(\mathbb{Q}) = \sum_{d|N} \phi_u(\gcd(d, N/d)).$$

Here  $\phi_u$  is the *reduced totient function*

$$\phi_u(n) := \# \left( \frac{(\mathbb{Z}/n\mathbb{Z})^\times}{\{\pm 1\}} \right) = \begin{cases} \frac{\phi(n)}{2} & \text{if } n \geq 3, \\ 1 & \text{if } n = 1, 2. \end{cases}$$

The second formula is for the number of orbits of  $\mathbb{P}^1(K)$  under the action of  $\mathrm{GL}_2(\mathcal{O}_K)$ , where  $K$  is a number field and  $\mathcal{O}_K$  is its ring of integers:

$$(1.2) \quad \#\mathrm{GL}_2(\mathcal{O}_K) \backslash \mathbb{P}^1(K) = h.$$

Here,  $h = h(K)$  is the size of the class group  $\mathrm{Pic}(\mathcal{O}_K)$ . Formula (1) is due to Bianchi. A formula counting the number of orbits of  $\mathbb{P}^1(K)$  under the action of congruence subgroups analogous to  $\Gamma_0(N)$  is given in [CA].

---

<sup>1</sup>Our definition of  $\Gamma_0(N)$  is not the traditional one, as we allow elements of determinant -1.

We can connect these two formulas using the theory of elliptic curves. For this, we let  $E$  and  $E'$  be elliptic curves over  $\mathbb{C}$ , and we consider the number  $N(E, E')$  of elliptic curves on the abelian surface  $A = E \times E'$  up to the action of  $\text{Aut}(A)$ . This number is finite by [LOZ], and in fact  $N(E, E') = 2$  unless there exists an isogeny  $\lambda : E \rightarrow E'$ . This raises the question, how do we compute  $N(E, E')$  if  $E$  and  $E'$  are isogenous?

If  $\text{End}(E) = \mathbb{Z}$ , then  $\text{Hom}(E, E') = \lambda\mathbb{Z}$ , for a certain minimal isogeny  $\lambda$ , whose degree we will denote by  $N$ . Then  $\text{Aut}(A) \simeq \Gamma_0(N)$  and we have  $N(E, E') = \#\Gamma_0(N) \backslash \mathbb{P}^1(\mathbb{Q})$  [RS, Prop. 3.7]. So the number  $N(E, E')$  is given by the first formula (1). On the other hand, if  $E$  has complex multiplication (CM) by an imaginary quadratic field  $K$ , we may think of  $\text{Aut}(A)$  as a subgroup of  $\text{GL}_2(K)$ . As before, we have  $N(E, E') = \#\text{Aut}(A) \backslash \mathbb{P}^1(K)$ ; see Lemma 3.1. In the special case where  $E = E'$  and  $\text{End}(E) = \mathcal{O}_K$ , we have  $\text{Aut}(A) \simeq \text{GL}_2(\mathcal{O}_K)$  and Bianchi's formula (1) gives  $N(E, E) = h$ .

Our main result is a formula for  $N(E, E')$  for any two elliptic curves  $E, E'$  with CM by  $K$ . Equivalently, we compute  $\#\text{Aut}(M) \backslash \mathbb{P}^1(K)$  for any lattice  $M \subset K^2$ . To state the result, we define the *conductor* of an elliptic curve  $E$ , with CM by  $K$ , to be the index of  $\text{End}(E)$  inside the ring of integers  $\mathcal{O}_K$ . Thus, if  $E$  has conductor  $c$ , then  $\text{End}(E)$  is isomorphic to  $\mathcal{O}_c$ , the unique subring of index  $c$  inside  $\mathcal{O}_K$ . Concretely, if  $E \simeq \mathbb{C}/\mathfrak{a}$ , for some lattice  $\mathfrak{a}$  in  $K$ , then  $c$  is the index of the ring of multipliers  $\{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\}$  in  $\mathcal{O}_K$ .

**Theorem 1.1.** *Let  $K$  be an imaginary quadratic field whose only roots of unity are  $\pm 1$ .<sup>2</sup> Suppose  $E$  and  $E'$  are elliptic curves with complex multiplication by  $K$  and of conductors  $c$  and  $c'$  respectively. Define  $f = \text{lcm}(c, c')$  and  $f' = \text{gcd}(c, c')$ . Then*

$$N(E, E') = \sum_{\ell|f} h_\ell \cdot \phi_u(f/\ell) \sum_{g|\ell} 2^{\omega(\ell/g)} r_K(f', g, f/\ell).$$

Here:

- $h_\ell = \#\text{Pic}(\mathcal{O}_\ell) = h \cdot \ell \prod_{p|\ell} (1 - \chi_K(p)/p)$ ,
- $\chi_K$  is the quadratic Dirichlet character associated to  $K$ ,
- $\omega(n)$  is the number of distinct prime factors of  $n$ , and
- $r_K(a, b, N)$  is the number of cyclic subgroups of order  $N$  of a fixed elliptic curve of conductor  $a$  such that the quotient has conductor  $b$ .

---

<sup>2</sup>There are analogous formulas for the two imaginary quadratic fields with more roots of unity, but we omit these cases for simplicity.

The mysterious quantity in our formula is the function  $r_K(a, b, N)$ . This is a 3-variable multiplicative function which is made completely explicit in Corollary 4.3. For each prime  $p$ , the values of  $r_K$  on powers of  $p$  depend only on how  $p$  splits in  $K$ , so the number  $N(E, E')$  depends only on the two integers  $c$  and  $c'$  and the values of  $\chi_K$  on primes dividing  $cc'$ . The explicit formulas for  $r_K(a, b, N)$  are complicated, but we may interpret these numbers as the number of walks on certain graphs called *p-isogeny volcanoes*. The structure of the  $p$ -isogeny volcano makes it easy to compute the numbers  $r_K(a, b, N)$ , just by looking at the graph (see Theorem 4.2). A script for computing  $N(E, E')$  in Sage is included with this document on arXiv.

As a corollary of Theorem 1.1, we obtain orbit counting formulas for large class of subgroups of  $\mathrm{GL}_2(K)$  which are commensurable with the Bianchi group  $\mathrm{GL}_2(\mathcal{O}_K)$ . Explicitly, if  $E = \mathbb{C}/\mathfrak{a}$  and  $E' = \mathbb{C}/\mathfrak{a}'$ , for lattices  $\mathfrak{a}$  and  $\mathfrak{a}'$  in  $K$ , then  $\mathrm{Aut}(E \times E')$  is isomorphic to the group:

$$\Gamma(\mathfrak{a}, \mathfrak{a}') := \left\{ \gamma \in \begin{pmatrix} \mathcal{O}_c & c\mathfrak{a}(f'\mathfrak{a}')^{-1} \\ c'\mathfrak{a}'(f'\mathfrak{a})^{-1} & \mathcal{O}_{c'} \end{pmatrix} : \det \gamma = \pm 1 \right\}.$$

We then have the following orbit counting formula:

**Corollary 1.2.**

$$\#\Gamma(\mathfrak{a}, \mathfrak{a}') \backslash \mathbb{P}^1(K) = \sum_{\ell|f} h_\ell \cdot \phi_u(f/\ell) \sum_{g|\ell} 2^{\omega(\ell/g)} r_K(f', g, f/\ell).$$

In favorable cases, the formula in Corollary 1.2 simplifies. For example, if  $\mathfrak{a} = \mathfrak{a}' = \mathcal{O}_f$ , then  $\Gamma(\mathfrak{a}, \mathfrak{a}') = \mathrm{GL}_2(\mathcal{O}_f)$  and the right hand side becomes a simple Dirichlet convolution:

**Corollary 1.3.** *For any  $f \geq 1$ ,*

$$\#\mathrm{GL}_2(\mathcal{O}_f) \backslash \mathbb{P}^1(K) = \sum_{\ell|f} h_\ell \cdot \phi_u(f/\ell).$$

*Proof.* See Section 4. □

These results have application to other counting problems in geometry. For example,  $\#\Gamma(\mathfrak{a}, \mathfrak{a}') \backslash \mathbb{P}^1(K)$  is the number of cusps on the hyperbolic 3-manifold  $\Gamma(\mathfrak{a}, \mathfrak{a}') \backslash \mathbb{H}^3$ . It is also the number of equivalence classes of contractions of the abelian surface  $A = E \times E'$ , in the sense of the minimal model program. Our formula can be used to study the asymptotics of these quantities as  $A$  varies, and would be helpful in individual computations as well.

The proof of Theorem 1.1 involves a careful study of Ext-groups in the category of products of elliptic curves with complex multiplication by  $K$ , or equivalently, in the category of lattices in imaginary quadratic

fields. These results (found in Section 2) are interesting in their own right and should find other applications.

**1.1. Acknowledgements.** The second author thanks Andrew Snowden for a helpful conversation. The second author was partially supported by NSF grant DMS-0943832.

## 2. EXTENSIONS OF CM ELLIPTIC CURVES

Fix an imaginary quadratic number field  $K \subset \mathbb{C}$ . A  $K$ -lattice is a free abelian subgroup  $L \subset K^n$  of rank  $2n$  (for some  $n$ ). The quotient  $\mathbb{C}^n/L$  is a complex torus, which is known to be algebraic.

**2.1. Singular abelian surfaces.** For context, we recall a basic fact about the abelian surfaces we are considering.

**Proposition 2.1** ([MS]). *Let  $A/\mathbb{C}$  be an abelian surface. Then the following are equivalent:*

- (1)  $A \simeq \mathbb{C}^2/\Lambda$ , with  $\Lambda$  a  $K$ -lattice, for some imaginary quadratic field  $K$ .
- (2)  $A$  is the product of two elliptic curves having CM by the same field  $K$ .
- (3)  $A$  is isogenous to a product of two elliptic curves having CM by the same field  $K$ .

If these equivalent conditions hold, we say that  $A$  is *singular* and that  $A$  has *CM by  $K$* .

**2.2. Rank 1  $K$ -lattices.** Recall that an *order* in the quadratic field  $K$  is a subring  $R \subset \mathcal{O}_K$  such that  $\text{Frac}(R) = K$ . Every order has the form  $R = \mathbb{Z} + f\mathcal{O}_K$  for a unique positive integer  $f$ , called the *conductor* of  $R$ . For each lattice  $L \subset K^n$ , the *ring of multipliers*  $R(L)$  is the order  $\{\alpha \in K : \alpha L \subset L\}$ . The conductor of  $L$  is defined to be the conductor of  $R(L)$ .

If  $\mathfrak{a} \subset K$  is a rank 1  $K$ -lattice, then  $\mathfrak{a}$  is projective as an  $R(\mathfrak{a})$ -module. Two rank 1  $K$ -lattices  $\mathfrak{a}$  and  $\mathfrak{a}'$  are *homothetic* if  $\mathfrak{a} = \gamma\mathfrak{a}'$  for some  $\gamma \in K^\times$ . The set of homothety classes of lattices of conductor  $f$  forms a group under multiplication of lattices, which is denoted  $\text{Pic}(\mathcal{O}_f)$ . The set of homothety classes of lattices in  $K$  is therefore in bijection with  $\coprod_{f \geq 1} \text{Pic}(\mathcal{O}_f)$ . If  $E = \mathbb{C}/\mathfrak{a}$ , then we define the conductor of  $E$ , denoted  $\text{cond}(E)$ , to be the conductor of  $\mathfrak{a}$ .

**Proposition 2.2.** *Let  $A$  be a singular abelian surface with CM by  $K$ . Then there is a positive integer  $f$  and a lattice  $\mathfrak{a} \subset K$  of conductor  $f'$  dividing  $f$  such that*

$$A \cong \mathbb{C}/\mathcal{O}_f \oplus \mathbb{C}/\mathfrak{a}.$$

Moreover, the integers  $f$ ,  $f'$  and the class  $[\mathfrak{a}] \in \text{Pic}(\mathcal{O}_{f'})$  are uniquely determined by these conditions. In particular,

$$A \mapsto (f/f', [\mathfrak{a}])$$

is a bijection between the set of isomorphism classes of singular abelian surfaces with CM by  $K$  and pairs  $(g, [\mathfrak{a}])$ , where  $g \geq 1$  and  $[\mathfrak{a}]$  is a homothety class of lattices in  $K$ .

*Proof.* Since  $A$  is singular with CM by  $K$ , we may write  $A = E \times E'$  with  $E = \mathbb{C}/\mathfrak{a}$  and  $E' = \mathbb{C}/\mathfrak{a}'$  for rank 1  $K$ -lattices  $\mathfrak{a}$  and  $\mathfrak{a}'$ . Let  $c$  and  $c'$  be the conductors of these elliptic curves. Then  $E \times E' \simeq \mathbb{C}/\mathcal{O}_f \times \mathbb{C}/\mathfrak{a}\mathfrak{a}'$ , where  $f = \text{lcm}(c_1, c_2)$ . Moreover, if two lattices  $\mathfrak{a}, \mathfrak{b} \subset K$  have multiplication by  $\mathcal{O}_f$ , then  $\mathbb{C}^2/(\mathcal{O}_f \oplus \mathfrak{a}) \simeq \mathbb{C}^2/(\mathcal{O}_f \oplus \mathfrak{b})$  if and only if  $\mathfrak{a}$  and  $\mathfrak{b}$  are homothetic (see [MS] or [K]).  $\square$

**2.3. Extensions of rank 1 lattices.** Let  $L_1, L_2 \subset K$  be lattices of conductors  $f_1$  and  $f_2$ , and let  $E_i = \mathbb{C}/L_i$  (for  $i = 1, 2$ ) be the corresponding elliptic curves. Suppose also that  $L_1 = \mathbb{Z} + \mathbb{Z}\tau_1$  and  $L_2 = \mathbb{Z} + \mathbb{Z}\tau_2$  for elements  $\tau_1$  and  $\tau_2$  of  $K$ ; up to homothety, we may always choose such a basis.

**Proposition 2.3.** [BL, I.5.7 and I.6.2] *The association*

$$z \mapsto \frac{\mathbb{C}^2}{\begin{pmatrix} \tau_2 & 1 & z & 0 \\ 0 & 0 & \tau_1 & 1 \end{pmatrix}}$$

*induces an isomorphism between the group  $\tilde{E} := \mathbb{C}/L_1L_2$  and the group  $\text{Ext}_{\text{an}}^1(E_1, E_2)$  of equivalence classes of extensions of complex tori. Under this bijection, the subgroup of torsion points in  $\tilde{E}$  corresponds to the subgroup  $\text{Ext}_{\text{alg}}^1(E_1, E_2)$  of algebraic extensions.*

**Remark** There is a similar result in [PR, Thm. 6.1], attributed to Lichtenbaum, but the result is not stated correctly there.

Proposition 2.3 shows that  $\text{Ext}_{\text{alg}}^1(E_1, E_2) \simeq (\mathbb{Q}/\mathbb{Z})^2$  as a group. But it is not clear which (or how many) extension classes correspond to some fixed abelian surface. The following theorem gives this extra information.

**Theorem 2.4.** *Let  $P \in \tilde{E}$  be a torsion point of order  $n \geq 1$ , and let*

$$0 \rightarrow E_2 \rightarrow S \rightarrow E_1 \rightarrow 0$$

*be the corresponding extension given by Proposition 2.3. Then*

$$S \simeq \mathbb{C}/\mathcal{O}_{nf} \oplus \tilde{E}/\langle P \rangle,$$

*where  $f = \text{lcm}(f_1, f_2)$ .*

In the proof, we consider several different notions of extension.

- For each positive integer  $F$  divisible by  $f$ , the lattices  $L_1$  and  $L_2$  can be considered as  $\mathcal{O}_F$ -modules, and we have the group  $\text{Ext}_{\mathcal{O}_F}^1(L_1, L_2)$  of extensions of  $\mathcal{O}_F$ -modules
- We have the group  $\text{Ext}^1(L_1, L_2)$  of extensions of  $K$ -lattices
- We have the group  $\text{Ext}_{alg}^1(\mathbb{C}/L_1, \mathbb{C}/L_2)$  of extensions of abelian varieties
- We have the group  $\text{Ext}_{an}^1(\mathbb{C}/L_1, \mathbb{C}/L_2)$  of extensions of complex tori.

An extension of modules determines an extension of  $K$ -lattices, which determines an extension of abelian varieties, which determines an extension of complex tori, so there is a sequence of group homomorphisms

$$(2.1) \quad \text{Ext}_{\mathcal{O}_F}^1(L_1, L_2) \xrightarrow{\gamma_1} \text{Ext}^1(L_1, L_2) \xrightarrow{\gamma_2} \text{Ext}_{alg}^1(\mathbb{C}/L_1, \mathbb{C}/L_2) \xrightarrow{\gamma_3} \text{Ext}_{an}^1(\mathbb{C}/L_1, \mathbb{C}/L_2).$$

It is not hard to see that  $\gamma_1$ ,  $\gamma_2$ , and  $\gamma_3$  are injective. It is well-known that  $\gamma_2$  is an isomorphism; indeed, there is an equivalence of categories between  $K$ -lattices and abelian varieties isogenous to a product of elliptic curves with CM by  $K$ . Proposition 2.3 implies the image of  $\gamma_3$  is the torsion subgroup of  $\text{Ext}_{an}^1(\mathbb{C}/L_1, \mathbb{C}/L_2)$ .

**Lemma 2.5.** *For any  $F$  divisible by  $f = \text{lcm}(f_1, f_2)$ , there is an isomorphism of  $\mathcal{O}_F$ -modules*

$$\text{Ext}_{\mathcal{O}_F}^1(L_1, L_2) \cong \frac{\text{Hom}_{\mathcal{O}_F}(L_1, L_2)}{\frac{F}{f} \text{Hom}_{\mathcal{O}_F}(L_1, L_2)}.$$

*Proof.* Choose an algebraic integer  $\omega$  with  $\mathcal{O}_K = \mathbb{Z} + \omega\mathbb{Z}$ ; then  $\mathcal{O}_F = \mathbb{Z} + F\omega\mathbb{Z}$ . Tensoring with  $\mathcal{O}_{f_1}$  induces a surjection  $\text{Pic}(\mathcal{O}_F) \rightarrow \text{Pic}(\mathcal{O}_{f_1})$ , so we can find a sublattice  $\tilde{L}_1 \subset L_1$  with ring of multipliers  $\mathcal{O}_F$  such that  $\mathcal{O}_{f_1} \cdot \tilde{L}_1 = L_1$ . Consider the following resolution of  $L_1$  by projective  $\mathcal{O}_F$ -modules:

$$0 \longleftarrow L_1 \xleftarrow{\varphi_0} \tilde{L}_1^2 \xleftarrow{\varphi_1} \tilde{L}_1^2 \xleftarrow{\varphi_2} \dots,$$

with

$$\varphi_0 = [1, -k\omega] \quad \text{and} \quad \varphi_1 = \varphi_2 = \dots = \begin{bmatrix} F\omega & -f_1 F\omega^2 \\ \frac{F}{f_1} & -F\omega \end{bmatrix}.$$

We apply the functor  $\text{Hom}(-, L_2)$  and examine the first coordinate to obtain

$$\begin{aligned} \text{Ext}_{\mathcal{O}_F}^1(L_1, L_2) &= \frac{\left\{ \alpha \in \text{Hom}_{\mathcal{O}_F}(\tilde{L}_1, L_2) : \mathcal{O}_{f_1} \alpha \subset \text{Hom}_f(\tilde{L}_1, L_2) \right\}}{\left\{ \frac{F}{f_1} \mathcal{O}_{f_1} \cdot \text{Hom}_{\mathcal{O}_F}(\tilde{L}_1, L_2) \right\}} \\ &= \frac{\text{Hom}_{\mathcal{O}_F}(L_1, L_2)}{\frac{F}{f} \text{Hom}_{\mathcal{O}_F}(L_1, L_2)}, \end{aligned}$$

where the second line follows from [K, Lem. 15].  $\square$

**Remark** This lemma holds if  $K$  is a *real* quadratic field as well.

**Corollary 2.6.** *The map  $\gamma_i$  of (2.3) takes  $\text{Ext}_{\mathcal{O}_F}^1(L_1, L_2)$  isomorphically onto the  $F/f$ -torsion in  $\text{Ext}^1(L_1, L_2)$ .*

*Proof.* Lemma 2.5 shows that  $\text{Ext}_{\mathcal{O}_F}^1(L_1, L_2)$  is an  $F/f$ -torsion group, so  $\gamma_1$  maps into the  $F/f$ -torsion in  $\text{Ext}^1(L_1, L_2)$ . Proposition 2.3 implies that the  $F/f$ -torsion in  $\text{Ext}_{\text{alg}}^1(\mathbb{C}/L_1, \mathbb{C}/L_2)$  has cardinality  $(F/f)^2$ , hence the  $F/f$ -torsion in  $\text{Ext}^1(L_1, L_2)$  also has cardinality  $(F/f)^2$  because  $\gamma_2$  is an isomorphism. Finally, we know  $\gamma_1$  is injective, and since its source and target have the same finite cardinality,  $\gamma_1$  must be an isomorphism.  $\square$

**Lemma 2.7.** *Suppose*

$$0 \rightarrow L_2 \rightarrow L \rightarrow L_1 \rightarrow 0$$

*is an extension of  $K$ -lattices, where  $L_i$  has conductor  $f_i$  (for  $i = 1, 2$ ). If the corresponding element of  $\text{Ext}^1(L_1, L_2)$  has order  $n$ , then  $L$  has conductor  $n \cdot \text{lcm}(f_1, f_2)$ .*

*Proof.* The conductor of  $L$  is the minimal  $F$  such that the class in  $\text{Ext}^1(L_1, L_2)$  representing  $L$  is in the image of  $\text{Ext}_{\mathcal{O}_F}^1(L_1, L_2)$ . Corollary 2.6 implies that this value is  $n \cdot \text{lcm}(f_1, f_2)$ .  $\square$

*Proof of Theorem 2.4.* The abelian surface  $S$  is given as  $\mathbb{C}^2/L$ , where  $L$  is the  $\mathbb{Z}$ -span of the period matrix in Proposition 2.3, with  $z \in \mathbb{C}$  any lift of the order  $n$  torsion point  $P \in \tilde{E} = \mathbb{C}/L_1 L_2$ . On the other hand, by Proposition 2.2, there is an integer  $N \geq 1$  and a lattice  $\mathfrak{a}$  with  $\mathcal{O}_N \subset R(\mathfrak{a})$ , such that  $L \simeq \mathcal{O}_N \oplus \mathfrak{a}$ . The conductor of  $\mathcal{O}_N \oplus \mathfrak{a}$  is  $N$ , so Lemma 2.7 implies  $N = nf$ .

We can recover  $\mathfrak{a}$  as the quotient of the group

$$\bigwedge_{\mathcal{O}_N}^2 (\mathcal{O}_N \oplus \mathfrak{a}) \cong \bigwedge_{\mathcal{O}_N}^2 \mathfrak{a} \oplus \bigwedge_{\mathcal{O}_N}^2 \mathcal{O}_N \oplus (\mathcal{O}_N \otimes_{\mathcal{O}_N} \mathfrak{a}) \cong \left( \bigwedge_{\mathcal{O}_N}^2 \mathfrak{a} \right) \oplus \mathfrak{a}$$

modulo it torsion. On the other hand, the torsion-free part of  $\bigwedge_{\mathcal{O}_n}^2 L$  is spanned by the  $2 \times 2$ -minors of the period matrix. Thus,  $\mathfrak{a}$  is the lattice generated by  $L_1 L_2$  and the element  $z$ , i.e., the lattice corresponding to the elliptic curve  $\tilde{E}/\langle P \rangle$ .  $\square$

### 3. PROOF OF THEOREM 1.1

Let  $A = E \times E'$  be a product of two elliptic curves with CM by the same imaginary quadratic field  $K$ , and suppose the conductor of  $A$  is  $f \geq 1$ . Then we may think of  $\text{Aut}(A)$  as a subgroup of  $\text{GL}_2(K)$ . The latter acts on  $\mathbb{P}^1(K)$  by fractional linear transformation.

**Lemma 3.1.** *The orbits on  $\mathbb{P}^1(K)$  under the action of  $\text{Aut}(A) \subset \text{GL}_2(K)$  are in bijection with the  $\text{Aut}(A)$ -orbits of elliptic curves contained in  $A$ .*

*Proof.* An elliptic curve  $E \subset A$  determines a 1-dimensional subspace  $T_0 E \subset T_0 A$ , and the map  $E \mapsto T_0 E$  is an  $\text{Aut}(A)$ -equivariant bijection between elliptic curves on  $A$  and 1-dimensional subspaces of  $T_0 A$ .  $\square$

Thus, to prove Theorem 1.1, it suffices to count the number  $N(E, E')$  of  $\text{Aut}(A)$ -equivalence classes of elliptic curves on the abelian surface  $A = E \times E'$ . By Proposition 2.2, we may assume  $E = \mathbb{C}/\mathcal{O}_f$  and  $E' = \mathbb{C}/\mathfrak{a}$ , where  $\mathfrak{a}$  has conductor  $f'$  dividing  $f$ . If  $F \subset A$  is an elliptic curve contained in  $A$ , then both  $F$  and the quotient  $A/F$  are elliptic curves with CM by  $K$ , and one has a short exact sequence of abelian varieties:

$$(3.1) \quad 0 \rightarrow F \rightarrow A \rightarrow A/F \rightarrow 0.$$

If  $F' \subset A$  is another elliptic curve with corresponding sequence

$$(3.2) \quad 0 \rightarrow F' \rightarrow A \rightarrow A/F' \rightarrow 0,$$

then  $F \subset A$  and  $F' \subset A$  are  $\text{Aut}(A)$ -equivalent if and only if (3) and (3) are isomorphic as short exact sequences.

**Lemma 3.2.** *If  $F \subset A$  is an elliptic curve, then the conductor of  $F$  divides  $f$ .*

*Proof.* Choose a map  $j : E \rightarrow A$  so that  $F = j(E)$ . Write  $j = (j_1, j_2)$  for maps  $j_1 : E \rightarrow E$  and  $j_2 : E \rightarrow \mathbb{C}/\mathfrak{a}$ . Since  $\mathcal{O}_f$  acts on both  $E$  and  $\mathbb{C}/\mathfrak{a}$ , we have  $\ker j_1 = E[I_1]$  and  $\ker j_2 = E[I_2]$  for certain ideals  $I_1$  and  $I_2$  of  $\mathcal{O}_f$ , by a result of Kani [K, Thm. 20(b)]. Here,  $E[I]$  is the subgroup of points in the kernel of  $\alpha : E \rightarrow E$  for every  $\alpha \in I$ . Thus,

$$\ker j = \ker j_1 \cap \ker j_2 = E[I_1] \cap E[I_2] = E[I_1 + I_2].$$



It follows that  $F \simeq E/\ker j \simeq E/E[I_1+I_2]$ , and so  $F$  has multiplication by  $\mathcal{O}_f$ .  $\square$

**Proposition 3.3.**  *$N(E, E')$  is equal to the number of isomorphism classes of short exact sequences*

$$0 \rightarrow E_1 \rightarrow A \rightarrow E_2 \rightarrow 0,$$

with  $E_1$  and  $E_2$  elliptic curves of conductor dividing  $f$ .

*Proof.* The previous lemma shows that any elliptic curve  $E_1 \subset A$  has conductor dividing  $f$ . Dualizing, we see that  $E_2 = A/E_1$  is also an elliptic curve on  $\hat{A} = A$ , so has conductor dividing  $f$  as well.  $\square$

We continue the proof of Theorem 1.1. Suppose that  $E_1$  and  $E_2$  are elliptic curves with conductor dividing  $f$ . Observe that if  $\gamma_1, \gamma_2 \in \text{Ext}^1(E_2, E_1)$  correspond to extensions

$$(3.3) \quad 0 \rightarrow E_1 \rightarrow A_1 \rightarrow E_2 \rightarrow 0,$$

$$(3.4) \quad 0 \rightarrow E_1 \rightarrow A_2 \rightarrow E_2 \rightarrow 0,$$

then (3) and (3) are isomorphic as short exact sequences if and only if  $\gamma_1$  and  $\gamma_2$  are in the same orbit of  $\text{Aut}(E_1) \times \text{Aut}(E_2)$  on  $\text{Ext}^1(E_2, E_1)$ . By assumption,  $K$  contains no non-trivial roots of unity, so  $\text{Aut}(E_1) = \text{Aut}(E_2) = \{\pm 1\}$ . Combining this observation with Proposition 3.3, we obtain

$$N(E, E') = \#\text{Aut}(A) \backslash \mathbb{P}^1(K) = \sum_{f_1, f_2 | f} \sum_{\substack{L_1 \in \text{Pic}(\mathcal{O}_{f_1}) \\ L_2 \in \text{Pic}(\mathcal{O}_{f_2})}} \#\text{Ext}_{\mathcal{O}_f}^1(L_2, L_1)_A / \{\pm 1\},$$

where  $\text{Ext}_{\mathcal{O}_f}^1(L_2, L_1)_A$  is the set of extensions classes  $0 \rightarrow L_1 \rightarrow L \rightarrow L_2 \rightarrow 0$  in  $\text{Ext}_{\mathcal{O}_f}^1(L_2, L_1)$  such that  $A \simeq \mathbb{C}^2/L$ .

Now fix integers  $f_1$  and  $f_2$  dividing  $f$ , and set  $g = \gcd(f_1, f_2)$ ,  $\ell = \text{lcm}(f_1, f_2)$ . Recall that an isogeny of elliptic curves is *cyclic* if its kernel is a cyclic group. We call a cyclic isogeny *based* if the kernel is equipped with a distinguished generator. By Theorem 2.4, classes in  $\text{Ext}_{\mathcal{O}_f}^1(L_2, L_1)_A$  correspond to based cyclic isogenies  $\mathbb{C}/L_1L_2 \rightarrow \mathbb{C}/\mathfrak{a}$  of degree  $f/\ell$ . Dualizing, we find that these are equinumerous to based cyclic  $(f/\ell)$ -isogenies  $\mathbb{C}/\mathfrak{a} \rightarrow \mathbb{C}/L_1L_2$ .

Recall that  $r_K(a, b, N)$  is the number of cyclic subgroups of order  $N$  of a fixed elliptic curve of conductor  $a$  such that the quotient has conductor  $b$ . Thus, there are  $r_K(f', g, f/\ell)$  cyclic subgroups  $G \subset \mathbb{C}/\mathfrak{a}$  of order  $f/\ell$  such that the quotient has conductor  $g$ . For each such subgroup, there are  $h_{f_1}h_{f_2}/h_g = h_\ell$  pairs  $L_1 \in \text{Pic}(\mathcal{O}_{f_1})$ ,  $L_2 \in \text{Pic}(\mathcal{O}_{f_2})$  with  $(\mathbb{C}/\mathfrak{a})/G \cong \mathbb{C}/L_1L_2$ . Given such  $G$ ,  $L_1$ , and  $L_2$ , there are  $\phi_u(f/\ell)$

based cyclic  $(f/\ell)$ -isogenies  $\mathbb{C}/\mathfrak{a} \rightarrow \mathbb{C}/L_1L_2$  with kernel  $G$ , up to the action of  $\{\pm 1\}$ . So we conclude that

$$\begin{aligned} \#\text{Aut}(A) \backslash \mathbb{P}^1(K) &= \sum_{\substack{k,d|f \\ g=\gcd(k,d) \\ \ell=\text{lcm}(k,d)}} h_\ell \cdot \phi_u(f/\ell) \cdot r_K(f', g, f/\ell) \\ &= \sum_{g|\ell|f} 2^{\omega(\ell/g)} \cdot h_\ell \cdot \phi_u(f/\ell) \cdot r_K(f', g, f/\ell), \end{aligned}$$

completing the proof of Theorem 1.1.

#### 4. COMPUTATION OF $r_K(a, b, c)$

To make Theorem 1.1 explicit, we need to compute the number  $r_K(a, b, c)$  of cyclic subgroups  $C$  of order  $c$  of a fixed CM elliptic curve  $E$  of conductor  $a$  such that  $E/C$  has conductor  $b$ . We will see that this does not depend on the choice of the elliptic curve  $E$  of conductor  $a$ . First we reduce to the case where  $a, b$ , and  $c$  are powers of a prime  $p$ :

**Lemma 4.1.** *The function  $r_K(a, b, c)$  is multiplicative: if we factor  $a$ ,  $b$ , and  $c$  into prime powers  $a = \prod_p p^{a_p}$ ,  $b = \prod_p p^{b_p}$ , and  $c = \prod_p p^{c_p}$ , then*

$$r_K(a, b, c) = \prod_p r_K(p^{a_p}, p^{b_p}, p^{c_p}).$$

*Proof.* If  $E$  is an elliptic curve, then giving a cyclic subgroup of order  $c$  is the same as giving a cyclic subgroup of order  $p^{c_p}$  for every prime  $p$ . Furthermore, if  $E \rightarrow E'$  is an isogeny of CM elliptic curves of  $p$ -power degree, the ratio of the conductors of  $E$  and  $E'$  is a power of  $p$ . To see this, it suffices to show that if  $\mathfrak{a} \subset \mathfrak{b}$  is an inclusion of rank 1  $K$ -lattices of index  $p^a$ , then the conductors of  $\mathfrak{a}$  and  $\mathfrak{b}$  are off by a power of  $p$ . And indeed, the  $\ell$ -part of the conductor can be computed locally at  $\ell$ , and  $\mathfrak{a} \hookrightarrow \mathfrak{b}$  induces an isomorphism  $\mathfrak{a} \otimes \mathbb{Z}_\ell \simeq \mathfrak{b} \otimes \mathbb{Z}_\ell$ , for all  $\ell \neq p$ . It follows then that

$$r_K(a, b, c) = \prod_p r_K(a, p^{b_p} \prod_{\ell \neq p} \ell^{a_\ell}, p^{c_p})$$

and

$$r_K(a, p^{b_p} \prod_{\ell \neq p} \ell^{a_\ell}, p^{c_p}) = r_K(p^{a_p}, p^{b_p}, p^{c_p}),$$

which proves the lemma.  $\square$

Next, we fix a prime  $p$  and show how to compute the numbers  $r_K(p^a, p^b, p^c)$ . We will use a variant of the  $p$ -isogeny volcano [S], a tool typically used to study isogenies of elliptic curves over finite fields. We define a graph  $G_p$ , called the *volcano*, whose structure depends only on  $p$  and  $\chi_K(p)$ , i.e. whether  $p$  is split, inert, or ramified in  $K$ . We omit the dependence on  $K$  in the notation. The vertices of  $G_p$  are partitioned into infinitely many *levels*  $G_{p,k}$ , one for each integer  $k \geq 0$ . We call the subgraph on  $G_{p,0}$  the *rim* of the volcano. The graph  $G_p$  is then uniquely determined by the following conditions:

- $G_p$  is  $(p+1)$ -regular, with no self-loops or multi-edges.
- The rim  $G_{p,0}$  is the complete graph on  $2 + \chi_K(p)$  vertices.
- For  $k \geq 1$ , each vertex in  $G_{p,k}$  has a unique neighbor in  $G_{p,k-1}$ , and this accounts for every edge not in the rim.

The figures below depict the top two levels of the graph  $G_3$  for each of the three splitting types.

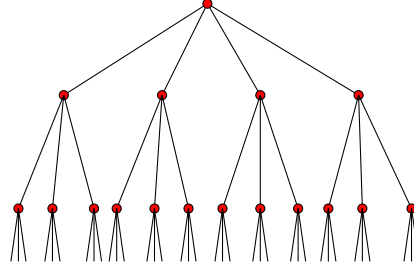


FIGURE 1.  $G_3$ , inert case.

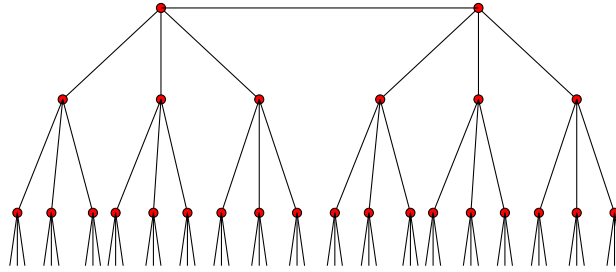
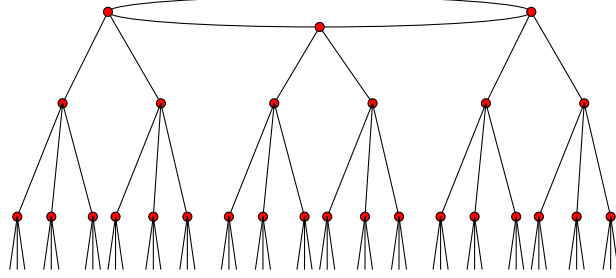


FIGURE 2.  $G_3$ , ramified case.

FIGURE 3.  $G_3$ , split case.

The vertices in  $G_p$  of level  $k$  are meant to correspond to elliptic curves with conductor equal to  $p^k$ . This is not a bijective correspondence however; the graph  $G_p$  is merely a convenient tool to understand the network of  $p$ -isogenies between CM elliptic curves.

Recall that if  $G = (V, E)$  is a graph, and  $v, v' \in V$  are vertices, then a *walk from  $v$  to  $v'$  of length  $c$*  is a sequence

$$v = v_0, e_1, v_1, e_2, \dots, v_{c-1}, e_c, v_c = v',$$

where each  $e_i \in E$  is an edge connecting  $v_{i-1}$  and  $v_i$ .

**Definition** A walk is called *non-backtracking* if  $e_i \neq e_{i+1}$  for all  $i$ .

**Theorem 4.2.** *Let  $a, b, c$  be non-negative integers. Then  $r_K(p^a, p^b, p^c)$  is the number of non-backtracking walks of length  $c$  in  $G_p$  starting at a fixed vertex of level  $a$  and ending at a vertex of level  $b$ .*

*Proof.* First consider the case  $c = 0$ . Then  $r_K(p^a, p^b, 1) = 0$  unless  $a = b$ , in which case it equals 1. This agrees with the fact that there are no walks of length 0 from a fixed vertex of level  $a$  to level  $b$ , unless  $a = b$ , in which case there is exactly one: the trivial walk.

Next consider the case  $c = 1$ . If  $E$  is an elliptic curve of conductor  $p^a$ , then  $E$  has  $p + 1$  subgroups  $C$  of order  $p$ , and Theorem 4.2 is claiming that the conductors  $\text{cond}(E/C)$  are exactly given by the levels of the  $p + 1$  neighbors of any vertex of level  $a$  in  $G_p$ . Specifically, if  $a = 0$ , the claim is that exactly  $1 + \chi_K(p)$  of these quotients have conductor 1, while the others have conductor  $p$ . And if  $a > 0$ , the claim is that exactly one of these quotients has conductor  $p^{a-1}$ , while the others have conductor  $p^{a+1}$ .

We give a short proof of these two facts using Kani's result [K, Thm. 20(b)] that a finite subgroup  $C \subset E$  is of the form  $C = E[I]$  for some ideal  $I \subset \text{End}(E)$  if and only if the conductor of  $E/C$  divides the conductor of  $E$ . Thus, if  $E$  has conductor 1, then exactly  $1 + \chi_K(p)$

subgroups of order  $p$  give rise to quotients of conductor 1, namely the subgroups of the form  $E[\mathfrak{p}]$  for an ideal  $\mathfrak{p} \subset \mathcal{O}_K$  of norm  $p$ . For the other subgroups  $C$ , the ring  $\text{End}(E/C)$  certainly contains  $\mathcal{O}_p = \mathbb{Z} + p\mathcal{O}_K$ , and so this containment must be a strict equality:  $\text{End}(E/C) = \mathcal{O}_p$ .

If  $E$  has conductor  $p^a$  with  $a > 0$ , then the non-Dedekind ring  $\text{End}(E) \simeq \mathcal{O}_{p^a}$  has exactly one ideal of norm  $p$ : the ideal  $I = p\mathcal{O}_{p^{a-1}}$ . If  $E \simeq \mathbb{C}/L$ , then  $E/E[I] \simeq \mathbb{C}/\mathcal{O}_{p^{a-1}}L$ , which has conductor  $p^{a-1}$ . Thus, by Kani's result,  $E$  has exactly one  $p$ -isogeny to a curve of conductor  $p^{a-1}$ , and no  $p$ -isogenies to curves of conductor  $p^a$ . The remaining  $p$  subgroups  $C$  have the property that  $\mathcal{O}_{p^{a+1}} = \mathbb{Z} + p\mathcal{O}_{p^a} \subset \text{End}(E/C)$ , but by the above, this inclusion must be an equality, i.e.  $E/C$  has conductor  $p^{a+1}$ . This proves the theorem in the case  $c = 1$ .

The general case  $c > 1$  follows immediately from the case  $c = 1$ , since every cyclic  $p^c$ -isogeny is a composition of  $p$ -isogenies. Composing  $p$ -isogenies amounts to taking walks along the isogeny volcano  $G_p$ . The condition that the walk is non-backtracking comes from the condition that the  $p^c$ -isogeny is cyclic. Indeed, backtracking amounts to composing with the dual of the previous  $p$ -isogeny, which would make the the composition divisible by  $p$  and hence not cyclic.  $\square$

Theorem 4.2 allows us to compute  $r_K(p^a, p^b, p^c)$  explicitly:

**Corollary 4.3.** *Let  $\chi_K(p)$  equal  $-1$ ,  $0$ , or  $1$ , depending on whether  $p$  is inert, ramified, or split in  $K$ . Then*

$$r_K(p^a, p^b, p^c) = \begin{cases} 0 & \text{if } a < b \text{ and } c < b - a \\ p^c & \text{if } 0 < a \leq b \text{ and } c = b - a \\ (p - \chi_K(p)) p^{c-1} & \text{if } 0 = a < b \text{ and } c = b \\ (p - 1)p^{(b-a+c)/2-1} & \text{if } a \leq b \text{ and } b - a < c < b + a \\ (p - \chi_K(p) - 1)p^{b-1} & \text{if } a \leq b \text{ and } c = b + a \\ (1 + \chi_K(p))(p - \chi_K(p))p^{b-1} & \text{if } a \leq b \text{ and } c = b + a + 1 \\ (\chi_K(p) + |\chi_K(p)|)(p - 1)p^{b-1} & \text{if } a \leq b \text{ and } c > b + a + 1 \\ r_K(p^b, p^b, p^{c-a+b}) & \text{if } a > b. \end{cases}$$

Here, we use the convention that  $p^s = 0$  if  $s$  is not an integer. Note that the formula in the last case reduces to one of the earlier cases.

**Remark** We will see in the proof that counting non-backtracking walks on  $G_p$  is quite easy; it is only the formulas which are complicated.

*Proof.* The structure of  $G_p$  makes it simple to compute the number of non-backtracking walks from level  $a$  to level  $b$  of length  $c$ . Indeed, once a non-backtracking walk descends down the volcano, then it can never reascend. So any non-backtracking walk starting at level  $a$  consists of

three stages. It begins by ascending up the volcano to some level  $k \leq a$ , and there is a unique way to do this.

If  $k = 0$ , then there is a middle stage where the walk may move horizontally along the rim. In the split case, this may involve circling around the rim many times, but the walk is not allowed to change directions (by the non-backtracking assumption). There are therefore two ways to perform this middle stage in the split case, no matter how many times the walk winds around the rim. In the ramified case, the walk may traverse the unique edge on the rim once, but then it is forced to move down the volcano, again by the non-backtracking assumption. In the inert case, this middle stage does not happen as there is a single vertex on the rim.

The final stage of the walk is the descent down the volcano from level  $k$  to level  $b$ . There are many ways to descend to level  $b$  but it is easy to count the number of possibilities. Note that there are two reasons a non-backtracking walk would ascend up the volcano initially: either to get to level  $b$  (if  $a < b$  for example), or to stall, in the event that going down to level  $b$  directly would result in a trip of length less than  $c$ . The corollary follows from consideration of the above analysis in each case, and writing the resulting formulas in terms of the character  $\chi_K$ .  $\square$

As an example of how to compute these numbers “by eye”, we now give the proof of Corollary 1.3. This is the special case where  $A = \mathbb{C}^2/\mathcal{O}_f^2$ , and hence  $\text{Aut}(A) = \text{GL}_2(\mathcal{O}_f)$ .

*Proof of Corollary 1.3.* We need to show that if  $g \mid \ell \mid f$ , then

$$r_K(f, g, f/\ell) = \begin{cases} 1 & \text{if } g = \ell \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 4.1, we may assume  $f = p^a$ ,  $g = p^b$ , and  $\ell = p^c$ , with  $a \geq c \geq b$ . Then if  $b < c$ , a vertex in level  $a$  cannot walk to level  $b$  in  $a - c$  steps. But if  $b = c$ , there is a unique (ascending) walk from a vertex of level  $a$  to a vertex of level  $b$  of length  $a - b$ , as claimed.  $\square$

In the general case, the formula for  $N(E, E')$  obtained by combining Theorem 1.1 and Corollary 4.3 does not seem to simplify much further.

## REFERENCES

- [BL] C. Birkenhake and H. Lange. *Complex Tori*. Springer, 1999.
- [CA] J. E. Cremona and M. T. Aranés. Congruence subgroups, cusps and manin symbols over number fields. In *Computations with Modular Forms*, pages 109–127. Springer, 2014.

- [LOZ] H. Lenstra Jr, F. Oort, and Y. Zarhin. Abelian subvarieties. *Journal of Algebra*, 180(2):513–516, 1996.
- [PR] M. Papanikolas and N. Ramachandran. A weil–barsotti formula for drinfeld modules. *Journal of Number Theory*, 98(2):407–431, 2003.
- [RS] J. Rosen and A. Shnidman. Néron-Severi groups of product abelian surfaces. 2014, arXiv: 1402.2233.
- [K] E. Kani, Products of CM elliptic curves. *Collect. Math.* **62** (2011), no. 3, 297–339.
- [MS] T. Mitani and T. Shioda. Singular abelian surfaces and binary quadratic forms. In: *Classification of Algebraic Varieties and Compact Complex Manifolds*. Lect. Notes Math. **412** (1974), 259 - 287.
- [S] A. Sutherland. Isogeny volcanoes. *The Open Book Series*, 1(1):507–530, 2013.